Introduction to Modern Cryptography

Benny Chor

Finite Groups, Rings, and Fields

Lecture 3 Part I

Tel-Aviv University

revised Feb. 5th, 2008
**Review - Commutative Groups**

**Definition:** A non-empty set $G$ with a binary operation $+$ (addition) is called a **commutative group** if

1. $\forall a, b \in G, a + b \in G$ (closure under $+$).
2. $\forall a, b, c \in G, (a + b) + c = a + (b + c)$ (associativity).
3. $\forall a, b \in G, a + b = b + a$ (commutativity).
4. $\exists 0 \in G$ such that $\forall a \in G a + 0 = a$ (neutral element).
5. $\forall a \in G, \exists b \in G, a + b = 0$ (existence of inverse).

Note that $+$ and $0$ are just symbols. In a multiplicative and/or non-commutative context, $\cdot$ and $1$ are often used instead.
Sub-groups

• Let \((G, +)\) be a group. \((H, +)\) is called a sub-group of \((G, +)\) if it is a group, and \(H \subset G\).

• **Claim:** Let \((G, +)\) be a finite group, and \(H \subset G\). If \(H\) is closed under \(+\), then \((H, +)\) is a sub-group of \((G, +)\).

• **Question:** What happens in the infinite case?

• **Lagrange Theorem:** If \((G, +)\) is a finite group and \((H, +)\) is a sub-group of it, then \(|H|\) divides \(|G|\).

• **Remark:** Lagrange theorem holds for non-commutative groups as well.
Order of Group Elements

- Let \( a^n \) denote \( a + a + \ldots + a \) (\( n \) times).
- We say that \( a \) is of order \( n \) if \( a^n = 0 \), but for every \( m < n \), \( a^m \neq 0 \).
- Euler theorem: In \( \mathbb{Z}_m^* \), the multiplicative group of \( \mathbb{Z}_m^* \), each element is of order at most \( \phi(m) \).
- We will omit the operation from the group notation \((G, +)\) when it is obvious.
Cyclic Groups

- **Claim:** Let $G$ be a group, and $a$ an element of order $n$. The set $\langle a \rangle = \{0, a, \ldots, a^{n-1}\}$ is a subgroup of $G$.
- $a$ is called the generator of $\langle a \rangle$.
- By Lagrange theorem, for every $a \in G$, the order of $a$ divides $|G|$.
- Fermat’s “little” theorem: For every $a \in \{1, \ldots, p - 1\}$, $a^{p-1} \mod p = 1$ (why does this hold?).
- If $G$ is generated by some $a$ then $G$ is called cyclic, and $a$ is called a primitive element of $G$.
- **Theorem:** For any prime $p$, the multiplicative group $\mathbb{Z}_p^*$ is cyclic.
- **Question:** How many primitive elements does $\mathbb{Z}_p^*$ have? If we know one, say $g$, can we characterize the others?
**Review (or maybe not) - Rings**

**Definition:** A non-empty set \( R \) with two binary operation \( + \) (addition) and \( \cdot \) (multiplication) is called a **commutative ring with identity** if

1. \( \forall a, b \in R, a + b, a \cdot b \in R \) (closure under \( +, \cdot \)).
2. \( \forall a, b, c \in R, (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c) \) (associativity of \( +, \cdot \)).
3. \( \forall a, b \in R, a + b = b + a, a \cdot b = b \cdot a \) (commutativity of \( +, \cdot \)).
4. \( \exists 0, 1 \in R \) such that \( \forall a \in R, a + 0 = a \cdot 1 = a \) (neutral elements w.r.t. \( +, \cdot \)).
5. \( \forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c \) (distributivity of \( + \) w.r.t. \( \cdot \)).
6. \( \forall a \in R \exists b \in R, a + b = 0 \) (existence of additive inverse).

Again, \( +, \cdot \) and \( 0, 1 \) are just symbols. Note that we did **not** require the existence of multiplicative inverses.
Definition: A non-empty set $F$ with two binary operation $+$ (addition) and $\cdot$ (multiplication) is called a field if

1. $\forall a, b \in F, a + b, a \cdot b \in F$ (closure under $+$, $\cdot$).
2. $\forall a, b, c \in F, (a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity of $+$, $\cdot$).
3. $\forall a, b \in F, a + b = b + a, a \cdot b = b \cdot a$ (commutativity of $+$, $\cdot$).
4. $\exists 0, 1 \in F$ such that $\forall a \in F a + 0 = a \cdot 1 = a$ (neutral elements w.r.t. $+$, $\cdot$).
5. $\forall a, b, c \in F, a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivity of $+$ w.r.t. $\cdot$).
6. $\forall a \in F \exists b \in F, a + b = 0$ (existence of additive inverse).
7. $\forall a \neq 0 \in F \exists c \in F, a \cdot c = 1$ (existence of multiplicative inverse).
A field is a commutative ring with identity where each non-zero element has a multiplicative inverse:

\[ \forall a \neq 0 \in F \exists c \in F, a \cdot c = 1. \]

The multiplicative inverse of \( a \) is also denoted \( a^{-1} \).

Equivalently, \((F, +)\) is a commutative (additive) group, and \((F \setminus \{0\}, \cdot)\) is a commutative (multiplicative) group.
Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \ldots + a_1 x + a_0$ be a polynomial of degree $n$ in one variable $x$ over a field $F$ (namely $a_n, a_{n-1}, \ldots, a_1, a_0 \in F$).

**Theorem:** The equation $f(x) = 0$ has at most $n$ solutions in $F$. (Such solution is called a root of $f(x)$.)

**Remark:** The theorem does not hold over rings with identity. For example, in $\mathbb{Z}_{24}$, the equation $6x = 0$ has six roots $(0, 4, 8, 12, 16, 20)$, not just one.
Polynomial Remainders

Let \( f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \ldots + a_1 x + a_0 \)
\( g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \ldots + b_1 x + b_0 \) be two polynomials in one variable \( x \) over a field \( F \) such that \( m \leq n \).

**Theorem:** There is a unique polynomial \( r(x) \) of degree smaller than \( m \), and another unique polynomial, \( h(x) \), both over \( F \), such that
\[ f(x) = h(x) \cdot g(x) + r(x) . \]

The polynomial \( r(x) \) is called the remainder of \( f(x) \) modulo \( g(x) \).
Polynomial Remainders: A Maple Example

The remainder is 0 (the zero polynomial) iff $g(x) | f(x)$. But if this is not the case, the remainder may be of degree $m - 1$, while $f(x)$ and $g(x)$ may or may not be relatively prime.
Finite Fields

**Definition:** A field $(F, +, \cdot)$ is called a finite field if the set $F$ is finite.

**Example:** As we already saw, $\mathbb{Z}_p$ denotes the set $\{0, 1, ..., p - 1\}$, where we define $+$ and $\cdot$ as addition and multiplication modulo $p$, respectively.

It is not hard to prove that $(\mathbb{Z}_p, +, \cdot)$ is a field iff $p$ is a prime. (try this!)

It is also possible to show that for any prime, $p$, $(\mathbb{Z}_p, +, \cdot)$ is the only finite field with $p$ elements. This means that any finite field with that many elements is essentially $(\mathbb{Z}_p, +, \cdot)$ (up to changing names).

**Question:** Are there any finite fields except $(\mathbb{Z}_p, +, \cdot)$?
The Characteristic of Finite Fields

Let \((F, +, \cdot)\) be a finite field. There must be a positive integer, \(n\), such that \(1 + 1 + \ldots + 1\) (\(n\) times) equals 0.

The minimal such \(n\) is called the characteristic of \(F\), \(\text{char}(F)\).

**Theorem:** For any finite field \(F\), \(\text{char}(F)\) is a prime number.
Galois Fields $GF(p^k)$

**Theorem:** For every prime power $p^k$ ($k = 1, 2, \ldots$) there is a unique finite field with $p^k$ elements (unique up to renaming). These fields are denoted by $GF(p^k)$. There are no finite fields with other cardinalities.

Évariste Galois (1811-1832)

(www.wqsb.qc.ca/philemon/pmessier/mathematicians.htm)

**Remarks:**

1. For $F = GF(p^k)$, $\text{char}(F) = p$.
2. $GF(p^k)$ and $Z_{p^k}$ are not the same!
Polynomials over Finite Fields

Polynomial equations and factorizations over finite fields can be quite different than their rationals/reals counterparts.

Examples from a Maple session:

```
> factor(x^6-1);  # over the rationals/reals
             (x - 1) (x + 1) (x^2 + x + 1) (x^2 - x + 1)
> p:=7;
             p := 7
> f := modp1(ConvertIn(x^6-1,x),p);
             f := (x^5 + 6) mod 7
> modp1(Factors(f),p)[2];  # list of factors and their multiplicities over GF(7)
[[x + 5 mod 7, 1], [x + 6 mod 7, 1], [x + 2 mod 7, 1], [x + 1 mod 7, 1], [(x + 4) mod 7, 1], [(x + 3) mod 7, 1]]
> p:=2;
             p := 2
> g := modp1(ConvertIn(x^6-1,x),p);
             g := (x^6 + 1) mod 2
> modp1(Factors(g),p)[2];  # list of factors and their multiplicities over GF(2)
[[x + 1 mod 2, 2], [(x^2 + x + 1) mod 2, 2]]
```

Over $GF(7)$, $x^6 - 1$ has six linear factors (btw, is this a coincidence?), while over $GF(2)$ the factorization is the same as over the rationals (given that $-1 = 1$).
Irreducible Polynomials

A polynomial is irreducible over $GF(p)$ if it does not factor in $GF(p)$. Otherwise, it is called reducible.

Maple example:

```maple
> p:=2;
p := 2
> f := modp1(ConvertIn(x^5+x^3+1,x),p);
f := (x^5+x^3+1) mod 2
> modp1(Factors(f),p)[2]; # list of factors and their multiplicities over GF(2)
[[ (x^5+x^3+1) mod 2, 1 ]]
> p:=5;
p := 5
> g := modp1(ConvertIn(x^5+x^3+1,x),p);
g := (x^5+x^3+1) mod 5
> modp1(Factors(g),p)[2]; # list of factors and their multiplicities over GF(5)
[[ (x^2+2x+3) mod 5, 1 ], [ (x^3+3x^2+2x+2) mod 5, 1 ]]

$x^5 + x^3 + 1$ is irreducible over $GF(2)$, but reducible over $GF(5)$.
Implementing $GF(p^k)$ Arithmetic

**Theorem:** Let $f(x)$ be an irreducible polynomial of degree $k$ over $GF(p)$.

The arithmetic of the finite field $GF(p^k)$ can be realized by the set of polynomials over $GF(p)$ whose degree is at most $k - 1$, where addition and multiplication are done modulo $f(x)$.

**Comment:** For every $p, k$ there are irreducible polynomials of degree $k$ over $GF(p)$. Furthermore, such polynomial can be found efficiently (random polynomial time in $\log p$ and $k$).
Example: Implementing $GF(2^5)$

By the theorem, the finite field $GF(2^5)$ can be realized as the set of degree 4 polynomials over $Z_2$, with addition and multiplication done modulo the irreducible polynomial $f(x) = x^5 + x^3 + 1$.

Remark: $f(x) = x^5 + x^3 + 1$ is not the only irreducible polynomial over $Z_2$. But it does not matter which (irreducible) one we take – they all give the same object, $GF(2^5)$.

The coefficients of polynomials over $Z_2$ are 0 or 1. So a degree $k - 1$ polynomial can be written down by $k$ bits. For example, with $k = 5$:

- $x^3 + x + 1$ is represented by $(0, 1, 0, 1, 1)$
- $x^4 + x^3 + x + 1$ is represented by $(1, 1, 0, 1, 1)$
Implementing Addition in $GF(p^k)$

In fields of characteristic 2, $1 + 1 = 0$, so addition corresponds to bit-wise XOR.

For example, $(x^3 + x + 1) + (x^4 + x^3 + x + 1)$ corresponds to $\begin{pmatrix}0 & 1 & 0 & 1 & 1\end{pmatrix} \oplus \begin{pmatrix}1 & 1 & 0 & 1 & 1\end{pmatrix}$,

which equals $\begin{pmatrix}1 & 0 & 0 & 0 & 0\end{pmatrix}$, so

$$(x^3 + x + 1) + (x^4 + x^3 + x + 1) = x^4.$$  

For fields of larger characteristic $p > 2$, the procedure is the same, only instead of XOR we do $\text{mod } p$ addition.
Implementing Multiplication in $GF(p^k)$

Multiplication has two stages. First stage is polynomial multiplication, which results in a polynomial of degree (at most) $2k - 2$. The second stage is computing the remainder of this polynomial modulo the defining, irreducible polynomial of degree $k$, $f(x)$, doing the computation mod $p$.

Maple example, in $GF(2^5)$, with $f(x) = x^5 + x^3 + 1$:

```maple
> p(x) := expand((x^3+x+1)*(x^4+x^3+x+1));
p(x) := x^7 + x^6 + 3 x^4 + 2 x^3 + x^5 + x^2 + 2 x + 1
> rem(p(x), x^5+x^3+1, x) mod 2;
1 + x
```

So $(0, 1, 0, 1, 1) \cdot (1, 1, 0, 1, 1)$ equals $(0, 0, 0, 1, 1)$.

For small size finite field, a lookup table is the most efficient method for implementing multiplication.
Example: Implementing $GF(2^5)$ with Maple

Again, we take the irreducible polynomial $f(x) = x^5 + x^3 + 1$.

```maple
> G32 := GF(2, 5, x^5 + x^3 + 1);
  G32 := $Z_2 [x] \triangleleft (x^5 + x^3 + 1)$

> a := G32[ConvertIn](x);  # slightly cumbersome notation
  a := x mod 2

> b := G32[^\^](a, 8);  # raising to power 8
> c := G32[^\^](a, 9);  # colon after statement suppresses printing

> G32[ConvertOut](b);  # back to regular representation
  x^4 + x^3 + x

> G32[ConvertOut](c);
  x^4 + x^3 + x^2 + 1

> d := G32[ConvertIn](x^3 + x + 1);
  d := (x^3 + x + 1) mod 2

> e := G32[^\^](d, 8):
> G32[ConvertOut](e);
  x^2 + x + 1
```
More Operations in $GF(p^k)$ with Maple

We continuing the previous slide, with the finite field $GF(2^5)$ represented using the irreducible polynomial $f(x) = x^5 + x^3 + 1$. We now check whether elements are primitive, namely if they are generators of the multiplicative group $GF^*(2^5)$.

```
> e:=G32[``^``](d,31):
> G32[ConvertOut](e);

> G32[isPrimitiveElement](a);
true

> G32[isPrimitiveElement](b);
true

> G32[isPrimitiveElement](c);
true

> G32[isPrimitiveElement](d);
true

> G32[isPrimitiveElement](e);
false
```